IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Arvind Ramaswamy et al.	§	Confirmation No.:	6801
Serial No.:	10/506,815	§	Group Art Unit:	2446
Filed:	04/11/2005	§	Examiner:	Farhad Ali
For:	Method And System For A Network Management Console	§	Docket No.:	200601202-5

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: September 17, 2009

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on July 23, 2009.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventors to Peregrine Systems, Inc., was recorded on December 12, 2005, at Reel/Frame 017328/0356. The Merger document from Peregrine Systems, Inc. to HPC was recorded on May 31, 2006, at Reel/Frame 017703/0668. The Assignment from HPC to HPDC was recorded on July 10, 2006, at Reel/Frame 017905/0174.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-19.
Claim cancellations:	None.
Added claim:	20.
Presently pending claims:	1-20.
Presently appealed claims:	1-20.

IV. STATUS OF THE AMENDMENTS

No claims were amended after the final Office action dated June 10, 2009.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable. The specification references are made to the application as filed by Appellants. Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element. Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

In accordance with the invention of claim 1, a data network management system[1] comprises a data communication means,[2] a database[3] and a data processing means.[4] The data network management system identifies unauthorized access to a data network service,[5] provided at a service node[6] in a data network,[7] by a user node[8] in said data network, said service node having an agent and having means for maintaining a user access list,[9] said user access list having at least one data network address corresponding to at least one user node in said data network.[10] The data communication means periodically polls said agent at said service node and retrieves a user access list from said agent, said

---

[1] Fig. 1 (110). Disclosure p. 7 line 1.

[2] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 1-3.

[3] Fig. 1 (230, 260). Disclosure p. 7 lines 22-24.

[4] Fig. 1 (110). Disclosure p. 6 line 25.

[5] Disclosure p. 9 lines 6-9.

[6] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 16-17.

[7] Fig. 1 (100). Disclosure p. 7 line 1.

[8] Fig. 1 (200, 210, 240, 250, 270, 280, 290). Disclosure p. 7 lines 22-25.

[9] Fig. 1, (230, 260, 300). Disclosure p. 8 lines 6-8, 12-13.

[10] Disclosure p. 8 lines 31-33.

user access list specifying which users have accessed said service node.[11] The database maintains an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node.[12] The data processing means detects unauthorized access to said service node by comparing said user access list to said authorized access list and updates said authorized access list based on the user access list retrieved from said agent.[13]

In accordance with the invention of claim 5, a method identifies unauthorized access to a data network service,[14] provided at a service node[15] in a data network,[16] by a user node[17] in said data network, said service node having an agent and having means for maintaining a user access list,[18] said user access list having at least one data network address corresponding to at least one user node in said data network and identifying a plurality of accesses to said service node.[19] The method comprises periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network.[20] The method further comprises comparing said user access list to an authorized access list[21] and determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access

---

[11] Disclosure p. 9 lines 3-9.

[12] Disclosure p. 8 lines 15-17.

[13] Disclosure p. 9 lines 15-20.

[14] Fig. 3. Disclosure p. 9 lines 6-9.

[15] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 16-17.

[16] Fig. 1 (100). Disclosure p. 7 line 1.

[17] Fig. 1 (200, 210, 240, 250, 270, 280, 290). Disclosure p. 7 lines 22-25.

[18] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 6-8.

[19] Disclosure p. 8 lines 31-33.

[20] Fig. 3 (470, 480). Disclosure p. 9 lines 3-9 and p. 11 lines 9-10.

[21] Fig. 3 (490). Disclosure p. 9 lines 15-20 and p. 11 lines 11-13.

list.[22] If said access was not authorized, the method further comprises initiating a notification process.[23]

In accordance with the invention of claim 13, a computer-readable medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor,[24] cause said processor to identify unauthorized access to a data network service,[25] provided at a service node[26] in a data network,[27] by a user node[28] in said data network, said service node having an agent and having means for maintaining a user access list,[29] said user access list having at least one data network address corresponding to at least one user node in said data network.[30] The computer-readable medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor, cause said processor to perform steps comprising periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network.[31] The steps further comprise comparing said user access list to an authorized access list[32] and determining if an access to said data network service was authorized based on comparing said user access list to the authorized access list.[33] If said access was unauthorized, the steps further comprise initiating a notification process.[34]

---

[22] Fig. 3 (500). Disclosure p. 9 lines 15-20 and p. 11 lines 13-14.

[23] Fig. 3 (520). Disclosure p. 11 lines 16-17.

[24] *Fig. 1 (110). Disclosure p. 6 lines 25-26.*

[25] Fig. 3. Disclosure p. 9 lines 6-9.

[26] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 16-17.

[27] Fig. 1 (100). Disclosure p. 7 line 1.

[28] Fig. 1 (200, 210, 240, 250, 270, 280, 290). Disclosure p. 7 lines 22-25.

[29] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 6-8.

[30] Disclosure p. 8 lines 31-33.

[31] Fig. 3 (470, 480). Disclosure p. 9 lines 3-9 and p. 11 lines 9-10.

[32] Fig. 3 (490). Disclosure p. 9 lines 15-20 and p. 11 lines 11-13.

[33] Fig. 3 (500). Disclosure p. 9 lines 15-20 and p. 11 lines 13-14.

[34] Fig. 3 (520). Disclosure p. 11 lines 16-17.

In accordance with the invention of claim 18, a computer for use in a data network[35] identifies unauthorized access to a data network service,[36] provided at a service node[37] in a data network,[38] by a user node[39] in said data network, said service node having an agent and having means for maintaining a user access list,[40] said user access list having at least one data network address corresponding to at least one user node in said data network.[41] The computer comprises a central processing unit[42] and a means for storing an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node.[43] The computer further comprises a data communication means for periodically polling said agent at said service node and retrieving a user access list from said agent,[44] said user access list specifying which users have accessed said service node;[45] and a data processing means for comparing said retrieved user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.[46]

---

[35] Fig. 1 (110). Disclosure p. 6 lines 25-26.

[36] Fig. 3. Disclosure p. 9 lines 6-9.

[37] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 16-17.

[38] Fig. 1 (100). Disclosure p. 7 line 1.

[39] Fig. 1 (200, 210, 240, 250, 270, 280, 290). Disclosure p. 7 lines 22-25.

[40] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 6-8, 12-13.

[41] Disclosure p. 8 lines 31-33.

[42] Fig. 1 (110). Disclosure p. 6 lines 25-26.

[43] Fig. 1 (110). Disclosure p. 8 lines 15-16.

[44] Fig. 1 (230, 260, 300). Disclosure p. 8 lines 1-3 and p. 9 lines 3-9.

[45] Fig. 1 (110), Fig. 3 (470, 480). Disclosure p. 9 lines 3-9 and p. 11 lines 9-10.

[46] Fig. 1 (110), Fig. 3 (490). Disclosure p. 9 lines 15-20 and p. 11 lines 11-13 and 17-19.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-20 are obvious under 35 U.S.C. § 103(a) over Dauerer et al. (U.S. Pat. No. 5,627,967) in view of Noy et al. (U.S. Pat. No. 6,539,540).

VII. ARGUMENT

A. Obviousness rejection of claims 1-20 over Dauerer in view of Noy

1. Claim 1

Claim 1 requires "said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network . . . " A database is also required for maintaining an authorized access list for the service node. The authorized access list specifies which users are authorized to access the service node. Claim 1 further requires "a data communication means for . . . retrieving a user access list from said agent." The user access list retrieved from the agent is then, per the claim, compared to an "authorized access list" to detect unauthorized accesses.

Dauerer instead discloses in Figure 1 a primary network node CPU 16 that manages and accesses a master file 12. Figure 1 also shows a network node 14. The Examiner presumably analogizes Dauerer's network node 14 to the claimed service node. However, Dauerer does not teach or even suggest that the network node contains a user access list of users that have accessed that node.

Further, in the Final Office Action p. 3 first paragraph, Examiner cites Dauerer at col. 3 lines 41-45 as purportedly teaching "said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network . . ." However, at the cited location, Dauerer teaches "creating a plurality of **lists of authorized users** . . . at least one list of the plurality of lists corresponding to each mini-disk . . ." (emphasis added) Even if the mini-disks taught by Dauerer are analogous to service nodes (which Appellants do not admit is proper), each mini-disk being associated with a list of **authorized users** fails to teach or suggest "maintaining a user access list . . . having at least one data network address corresponding to at least one user node . . ." as required by the claimed limitation. That is, Dauerer's lists of authorized

users do not include network addresses; indeed, Dauerer does not mention using a "network address" nor an "address" as part of a user access list.

Further still, claim 1 requires the service node to contain an agent that is accessed by the data communication means to retrieve the user access list. Appellants find no mention in Dauerer of such an agent.

Claim 1 further requires the data processing means to detect unauthorized access to the service node by comparing the user access list to the authorized access list. The Examiner pointed to Dauerer at col. 7 line 55 as allegedly teaching the claimed comparison. However, that passage of Dauerer teaches comparing a new list against the previous version of that list. The comparison is not for the purpose of detecting, and thus does not detect, unauthorized access to the network node 14. Further, the comparison is not between a list of users that have actually accessed the node 14 and a list of users that are authorized to access the node 14.

Finally, in the Final Office Action beginning at p. 19 last paragraph, the Examiner disagrees with Appellants' prior argument that Dauerer does not teach or even suggest that the Network node contains a user access list of users that have accessed the node, and that this is compared to the authorized access list and cites Dauerer col. 5-6 lines 36-9 in support of Examiner's position. However, the Examiner mischaracterizes the cited portion of Dauerer. In the previous paragraph, col. 5 lines 25-27, Dauerer teaches that "the master list is processed at 204" by first identifying all duplicate user identifications. Thus, checking for invalid user identifications, which is performed "only when no duplicate user identifications are detected", is merely a step involved in processing the master list of Dauerer. Processing a master list by eliminating invalid user identifications fails to teach or even suggest maintaining a user list that is compared to an authorized access list to identify unauthorized access to a data network service as required by the claimed limitation.

Noy does not satisfy the preceding deficiencies of Dauerer. The Examiner used Noy (citing col. 1 lines 30-32) for allegedly teaching periodically polling an agent in a service node to retrieve a user access list. At the location cited by Examiner, Noy says that "an SNMP manager will periodically poll an agent in order to detect changes in the MIB information for a particular network device." Appellants do not find any teaching in Noy as to what sort of changes in MIB information are to be detected by polling the agent. The cited passage of Noy does not teach or even suggest retrieving a user access list from an agent.

Further, in Final Office Action beginning at p. 21 first full paragraph, Examiner asserts that "Noy is relied upon for the teaching of periodic polling . . ." However, in Final Office Action p. 4 first paragraph, Examiner asserts that "Dauerer et al. fails to teach a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said node." Appellants agree with this assertion. Dauerer fails to teach the claimed limitation and Noy fails to teach what sort of changes in MIB information are to be detected by polling the agent and specifically does not teach "a means for . . . retrieving a user access list from said agent.". Thus, none of the art of record teaches a means for retrieving a user access list from an agent.

For at least these reasons, the Examiner erred in rejecting claim 1 and its dependent claims over Dauerer in view of Noy.

2. Claim 5

Claim 5 requires retrieving a user aces list from a service node. The Examiner concedes Dauerer lacks this limitation, and, as explained above, Noy also lacks this limitation. Claim 5 also requires "determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list." As explained above, Dauerer lacks such a comparison. Further still, Dauerer lacks a service node having an agent and user access list as required by claim 5. For at least these reasons, the Examiner erred in rejecting claim 5 and its dependent claims over Dauerer in view of Noy.

3. Claim 6

Dependent claim 6 requires updating the authorized access list based on said user access list retrieved from the service node. Dauerer lacks any teaching whatsoever of updating a user access list "based on said user access list retrieved from said service node." While Dauerer may teach updating the master list, such an update is not based on a user access list retrieved from the network node 14. For at least this additional reason, the Examiner erred in rejecting dependent claim 6.

4. Claim 13

The Examiner erred in rejecting claim 13 for some or all of the same reasons specified above. All claims dependent on claim 13 are thus also in condition for allowance.

5. Claim 14

The Examiner erred in rejecting dependent claim 14 for the same or similar reasons as for claim 6.

6. Claim 18

Claim 18 has been amended to clarify what is meant by the user access and authorization lists. Thus, the Examiner erred in rejecting claim 18 and its dependent claims for some or all of the reasons expressed above regarding claim 1.

B. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees

required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Jonathan M. Harris/

Jonathan M. Harris
PTO Reg. No. 44,144
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528-9599

VIII. CLAIMS APPENDIX

1. A data network management system for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent, said user access list specifying which users have accessed said service node;

a database for maintaining an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node; and

a data processing means for detecting unauthorized access to said service node by comparing said user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.

2. The data network management system as defined in claim 1, wherein said agent is a Simple Network Management Protocol agent.

3. The data network management system as defined in claim 1, wherein said data communication means is a Simple Network Management Protocol communication means.

4. The data network management system as defined in claim 1, further including means for installing said agent at said service node, said agent having means to communicate with said data communication means.

5. A method for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, said method comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network;

b) comparing said user access list to an authorized access list;

c) determining if an access to said service node was unauthorized based on comparing said user access list to the authorized access list; and

d) if said access was not authorized, initiating a notification process;

wherein said user access list identifies a plurality of accesses to said service node.

6. The method as defined in claim 5, further including updating said authorized access list based on said user access list retrieved from said service node.

7. The method as defined in claim 5, further including installing said agent at said user node, prior to periodically polling and retrieving said user access list.

8. The method as defined in claim 5, further including selecting said service node for identification based on a predetermined criteria, prior to retrieving said user access list.

9. The method as defined in claim 5, wherein said notification process comprises notifying a Network Operations Console.

10. The method as defined in claim 5, wherein a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

11. The method as defined in claim 5, wherein a) through d) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

12. The method as defined in claim 5, wherein said agent is a Simple Network Management Protocol agent.

13. A computer-readable medium for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network, and said medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor, cause said processor to perform steps comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in a data network;

b) comparing said user access list to an authorized access list;

c) determining if an access to said data network service was authorized based on said comparison step b);

d) if determined that said access was unauthorized, initiating a notification process.

14. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information.

15. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a).

16. The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network.

17. The computer-readable medium as defined in claim 13, wherein said agent is a Simple Network Management Protocol agent.

18. A computer for use in a data network for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network, said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network; said computer comprising:

means for storing an authorized access list for said service node, said authorized access list specifying which users are authorized to access said service node;

a central processing unit;

data communication means for periodically polling said agent at said service node and retrieving a user access list from said agent, said user access list specifying which users have accessed said service node; and

data processing means for comparing said retrieved user access list to said authorized access list and for updating said authorized access list based on the user access list retrieved from said agent.

19. The data network as defined in claim 1, wherein said authorized access list is a common authorized user access list that includes a range of user nodes for comparing to said user access list to determine if said user access list is a subset of said common authorization access list.

20. The data network management system of claim 1 wherein said user access list identifies a plurality of accesses to said service node.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.